(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 January 2002 (24.01.2002)

PCT

(10) International Publication Number
WO 02/06948 A1

(51) International Patent Classification[7]: G06F 7/00, 11/30, 12/14, 17/30, H04K 1/00, H04L 9/00, 9/32

(21) International Application Number: PCT/US01/22089

(22) International Filing Date: 13 July 2001 (13.07.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/217,955 13 July 2000 (13.07.2000) US

(71) Applicant: **DIGINEER, INC.** [US/US]; 6847 Cintas Boulevard, Mason, OH 45040 (US).

(72) Inventors: **BEECH, Robert, P.**; 10064 Whitebridge Court, Cincinnati, OH 45242 (US). **AMFAHR, Jeffrey, A.**; 2791 Millstone Court, Maineville, OH 45039 (US). **BARKER, Randall, K.**; Box 271 Washington Trace Road (RR#1), California, KY 41007 (US). **MARTIN, Ted, T.**; 7645 Trailwind Drive, Cincinnati, OH 45242 (US). **MCCOOL, James, C.**; 10580 Schiller Road, Medway, OH 45341 (US).

(74) Agents: **LEVY, Mark, P.** et al.; Thompson Hine LLP, 2000 Courthouse Plaza N.E., 10 West Second Street, Dayton, OH 45202-1758 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/06948 A1

(54) Title: METHOD FOR PROTECTING THE PRIVACY, SECURITY, AND INTEGRITY OF SENSITIVE DATA

(57) Abstract: Methods for creating, storing, and viewing confidential data records are provided. Steps included in one embodiment of the invention include separatng a record into first and second files, generating a first key associated with the first file, storing the first file and the key in a first database, transmitting the second file and the first key over a network for storage in a second database, generating a second key derived from the first key and associating the second key with the second file and storing the second file in second database using the second key to index the second file. Other embodiments of the invention include steps for viewing, creating and storing confidential information using portable electronic hand held devices.

Method for Protecting the Privacy, Security, and Integrity of Sensitive Data

FIELD OF THE INVENTION

The present invention relates to information security, and more particularly to a method for protecting the privacy, security and integrity of confidential, individually identifiable, personal information and for facilitating the creation, use and access to this information over a secure public or private network or, where applicable, through portable electronic hand held devices (HHD's).

BACKGROUND

Many activities in which individuals engage result in the creation, transmission, and storage of potentially sensitive, individually identifiable information. While individuals generally wish to keep personal information secure and private from unauthorized users thereof, at times it may be desirable to provide authorized access to such personal information. Such access will generally require that the authorized user have the ability to use, view, and modify the information as necessary pursuant to their granted authorization. Representative examples of such situations include the authorized access granted to healthcare providers to use and modify healthcare records, as well as the authorized access granted to financial institutions to use and modify specific financial records.

Thus, while individuals may wish to allow duly authorized users of their personal information the ability to access such information as quickly and conveniently as possible, they would also like to protect the same information from use and abuse by unauthorized users. And as is well known in the industry, these two goals, while not necessarily mutually exclusive, can create a conflict that is sometimes difficult to resolve. In particular, it is well known in the information management field that increasing the accessibility of information almost always decreases the security thereof. The converse, namely that increased security levels generally result in decreased accessibility to the information, is almost always true as well. While this dichotomy has always presented problems in the field of information management and the security of the managed information, recent technological improvements have magnified this problem.

This concern about third parties' access to and misuse of their individually identifiable health data coincides with a transition from primarily paper-based to digital

information systems. The expanded use of digital information has resulted in significant and tangible organizational and societal benefits. For example, in the health care context, the transition to digital information systems has resulted in an increased ability to detect and treat disease, to conduct invaluable scientific research, to lower costs, and to improve overall the quality of care. At the same time the transition from paper-based to electronic systems also has given rise to new threats to the privacy of an individual's personal information. While the risk always has existed that someone would gain unauthorized access to personal information and then wrongfully disclose that information to others, that risk was relatively localized. However, the collection of this data in large electronic databases combined with the ability to transfer this data instantaneously around the world over public networks like the Internet or through "over air" transmissions to HHD's has exponentially increased the risk of exposure of sensitive, personal information.

In particular, the use of HHD's to create, send, and receive sensitive data can present specific problems with respect to maintaining the security of that data. In this regard, a background discussion of what is meant by "HHD" as used herein would be considered useful. As is known in the art, these devices come in a variety of sizes, shapes, capabilities, etc., and are available from an ever increasing number of manufacturers, one of the most famous being Palm Pilot. With respect to the various HHD's available now and in the future, the discussion herein is generally applicable to all devices that are characterized by their generally small size, making them easily portable, and their ability to receive, modify, and send data wirelessly using cellular or other "over air" wireless technologies. Other options that exist on many currently available HHD's include security features such as encryption and password technology and the ability to upload and download information between the HHD and a PC or workstation. It can even be contemplated that further innovations in this technology will result in the availability of additional features including security features that would require the inputting of a "biometric" response from the authorized user to gain access to any information contained in the HHD. Such improvements, while not specifically enumerated herein, could possibly be used in a manner consistent with the present invention and are therefore considered within the scope thereof.

Of course, while these HHD's facilitate accessibility to all types of information, their use also presents some rather unique security problems. In particular, given their small size and portability, HHD's are generally carried with the authorized user at all

times. Accordingly, HHD's are much more liable to be lost or stolen than the traditional PC or workstation. This presents a heretofore unseen security problem in that once the HHD is no longer in the possession of the authorized user, information that is stored in the HHD could be breached and misused in any number of ways. Furthermore, even if such stored information is encrypted and password protected, it is assumed that such security techniques could eventually be circumvented. The potential for a security breach increases exponentially in situations where the HHD is stolen by someone with the nefarious intent of abusing the information. Furthermore, even if the HHD were to fall into the hands of only a mere miscreant, the potential for abuse, and resultant damage to the individuals to whom the information pertains, still exists.

HHD's also present unique security risks compared to "hard-wired" PCs in their very nature in that their portability and convenience depends upon their use, and reliance upon, over air transmissions to receive, modify and send information. As opposed to hard-wired connections, over air transmissions tend to be inherently insecure in that transmissions to and from HHD's using over air transmission technologies can be intercepted without the need for actual "physical" access to the transmission network. Thus, even if the primary network in which the HHD is being used is a secure, hard-wired network, the potential still exists for the interception of transmissions directly to and from the HHD that bypass the hard-wired network.

Accordingly, concerns over complying with the privacy laws and regulations mentioned above, as well as other issues, such as reducing potential tort liability, mitigating the public privacy concerns mentioned above, and overall risk management have presented a very real need for a method for protecting the privacy, security and integrity of potentially sensitive, individually identifiable personal information in a manner in which authorized access to the information is facilitated over a secure public or private network or through "over air" transmissions to and from HHD's.

SUMMARY OF THE INVENTION

The present invention provides a method for protecting the privacy, security and integrity of confidential, individually identifiable, personal information and for facilitating the creation, use and access to this information over a secure public or private network or, where applicable, through an HHD.

While the present invention may be particularly useful in the healthcare and financial fields, the invention may be generally useful in any application wherein secure access to sensitive data is required. Users of the present invention could include health care providers, health clinics, patients, financial institutions, users of financial services, as well as others that create, store, retrieve, modify, provide, or otherwise use, sensitive data.

Initially it is noted that, as used herein, "over air" transmission refers to the transmission of information via RF, cellular, or other types of non-localized over air transmissions. Please note that the term "over air" as used herein to discuss transmission networks does not generally refer to "localized" non-hard-wired transmission networks, such as "bluetooth"-type transmission networks. In this regard, localized bluetooth-type transmission networks can be distinguished from other over air transmission networks in that their transmission range is so small as to render it practically impossible to intercept such a transmission without direct or very close physical access to the source of the transmission. As used herein, and as will be discussed in detail below, the term "authorized user" generally refers to the person who has been given authorization, either express or implied, to access and modify the relevant information. As used herein, the term "issuer" generally refers to the entity that validates the authorized user's right to access, generate and/or modify information. As used herein, the term "originator" generally refers to the entity that updates or modifies highly sensitive information (referred to below as de-identified data) and forwards that information, either directly or through the issuer, to the authorized user for review, comment or modification.

For example, in the healthcare context, the authorized user may be the healthcare provider who is given access to generate or modify individually identifiable information pertaining to a patient, such as patient records, test results, etc.; the issuer may be the hospital who gives and monitors those access rights; and the originator may be the lab that produces the test results. Alternatively, in a financial setting, the authorized user may be a loan officer who is given access to generate or modify individually identifiable information pertaining to a loan applicant, such as financial records, employment history, etc.; the issuer may be the financial institution, such as a bank, that gives and monitors those access rights; and the originator may be a credit institution that holds information about the authorized user.

In discussing the invention, it is to be understood that most sensitive data can generally be split into at least two separate components, namely, identified data and de-

identified data. Of course it is to be understood that the data could be separated into as many different components as desired and each component could be treated on the basis of the information contained in each component. For example, the data could be separated into three components, wherein one component would be identified data such as the name and address of a credit card holder, and the other two components could be related, but separate, de-identified data such as separate parts of a credit card number corresponding to the credit card holder identified by the identified data. In this regard, it is clear that none of the separate components, standing alone, would represent a significant security risk if intercepted by an unauthorized user. However, by associating all three data components either in a hard-wired PC in accordance with the method of the present invention disclosed below, an authorized user would be able to view, use and modify the information with a relatively minimal risk that the security of the information would be breached. Accordingly, even though the only embodiments discussed in detail below involve the use of only two separate types of data components, it is contemplated that the number of data components that could be used in accordance with the method of the present invention could be essentially unlimited. Thus, it is to be understood that the two data component embodiment disclosed below is discussed in detail for illustrative purposes only, and embodiments of the invention with more than two data components could easily be practiced by one of ordinary skill in the art without departing from the scope and claims of the present invention.

In an illustrative embodiment of a two data component system, the first component may be referred to as the identified data. In this embodiment, the identified data may generally consist of non-sensitive information, and is usually information that can be used directly or indirectly to identify the person who is the subject of the information (such as name, address, phone number, etc.) but is not generally information that, in and of itself, would be considered highly sensitive. The identified data is usually relatively static, not needing frequent updates or modifications thereto. The de-identified data is usually general information (such as clinical medical data, financial information, portions of credit card numbers, etc.) that is only highly sensitive if it can be matched with its corresponding identified data to form a combined record. The de-identified data generally consists of dynamic information that needs to be viewed, modified, or added to frequently.

One manifestation of the invention is a method for protecting confidential data records comprising the steps of:

separating a record into first and second files;

generating a first key associated with said first file;

storing said first file and said first key in a first database;

transmitting said second file and said first key over a network for storage in a second database;

generating a second key derived from said first key and associating said second key with said second file; and

storing said second file in a second database using said second key to index said second file.

In one particularly advantageous embodiment of the invention, the first and second databases are maintained by independent entities which are not under common control or ownership. Typically the first file will be that portion of the data record which identifies the individual or entity to which the information relates and the second file will be the balance of the record. In one particular application of the invention the data records are health care records. The method of the invention provides a secure method for accessing and/or transmitting data records over a private or public network such as the Internet. Security is achieved in part by independently generating linking keys using user-specific data or keys at the first and second database management locations and storing the data using the linking keys. As explained in more detail below, in this way the data records cannot be reconstructed from the first and second files unless the user has access to the algorithms that are used to generate the linking keys. If these algorithms are independently controlled, the likelihood of unauthorized reconstruction of the data records is minimized.

In one embodiment, data is created and stored in the following manner. The authorized user accesses software, at the point of service (such as a health care facility) or a trusted intermediary (such as a web site), by providing two pieces of identification (keys) to the authentication software: an authorized user access key and an authorized user verification key (e.g., a password). The authorized user is authenticated and is then allowed to perform further functions. The authentication software can be run in an otherwise conventional manner on an independent server or can be integrated with software that handles additional features in a common server, as in the case of the

illustrated embodiment of the invention wherein the multi-function software is referred to as the access software.

In either embodiment, following authentication the authorized user generates individually identifiable information. The access software divides this information into two components: 1) information that can be used directly or indirectly to identify the person who is the subject of the information, referred to here as "identified data" and 2) all of the remaining information, referred to here as "de-identified data." Those skilled in the art will recognize that the information could be divided into additional components if desired.

The identified data is preferably transmitted to an entity that stores identified data (referred to here as an "identified data service provider"). One way this can be accomplished securely is the following: the access software establishes secure communications with software operating at the site of an entity that stores identified data. This software is referred to as "identified data software". The access software transmits the identified data to the identified data software along with additional information for generating a key which will be used to link the identified data with the de-identified data as described below. In one embodiment this information is: the authorized user access key, the authorized user verification key, and a key that is unique to the issuer (referred to here as the "identified issuer key"). The identified data software authenticates the authorized user then generates a key associated with the identifying data using a process such as a random key generation process that creates unique keys. This key is referred to here as the " identifying linking key" or "ILK". One process creates the ILK using a restricted algorithm and the identified issuer key, the authorized user access key, the authorized user verification key, and a random number. The identified data and ILK are stored in the identified data database. The identified data software also transmits the ILK back to the access software. The identified data software updates an access list of the records to which the authorized user has access and the related ILKs of those records. While the ILK is described herein as being generated from the authorized user access key, the authorized user verification key and the issuer key, those skilled in the art will recognize that alternative authorized user and/or issuer specific data could alternatively be used to generate the ILK.

In another embodiment of the invention, the identified data may be stored at the point of service or with the intermediary. This practice will not be as secure as

transmitting the data to an identified service provider because the identified data software and the algorithm which it includes for generating the ILK will be on the same computer or a computer located at the same site as the access software.

The de-identified data is transmitted to a separate entity that stores the de-identified software (referred to here as the "de-identified data service provider" or "DDSP"). In one embodiment this is accomplished in the following manner. The access software transmits the de-identified data to software operating at the de-identified data service provider along with additional information such as the authorized user access key, the authorized user verification key, the ILK, and a de-identified data key that is unique to the issuer (referred to here as the "De-identified Issuer Key") to generate a key for indexing the de-identified data. The de-identified data software authenticates the authorized user. Using information such as the authorized user access key, the authorized user verification key, the ILK, the de-identified issuer key, and a restricted algorithm, the de-identified software creates a separate linking key, referred to here as the de-identified linking key (DILK). The DILK is used to index the stored de-identified data. Alternatively, the ILK could be used in combination with alternative authorized user and/or issuer specific data to generate the DILK.

In embodiments of the invention consistent with the data storage and retrieval method discussed above, access to combined identified and de-identified records using an HHD may be made by using: a method wherein the separate identified and de-identified data are never sent or transmitted to or from the HHD in combined form; a method wherein identified and de-identified data are transmitted only a single record at a time; and a method wherein the only relevant data stored on the HHD in persistent memory is relatively innocuous identified data. In another embodiment of the invention, only de-identified data is sent to the HHD and the corresponding identified data cannot be accessed from the HHD wirelessly. Please note, however, that in all of the embodiments of the invention wherein an HHD is utilized, it is a requirement that combined records can only be viewed and modified on the HHD in non-persistent memory. Accordingly, one embodiment of the present invention provides heretofore unknown security for the viewing and modification of sensitive combined records, or the viewing of "anonymous" de-identified data, using an HHD in that even the HHD is lost or stolen, an unauthorized user thereof can only access the relatively innocuous identified data that is stored therein. Furthermore, as will be discussed in detail below, unauthorized access to the identified

data is limited and subject to security protocols that can be used to protect the extent of any further security breach.

Specifically, in order to practice an embodiment of the method of the present invention utilizing an HHD, the authorized user has, or is issued, an HHD capable of receiving RF, cellular, or other over air transmissions. In addition to the HHD's over air receiving, and potentially transmitting, capabilities, the HHD used by the authorized user may be equipped with uplinking/downlinking capabilities allowing the HHD to be connected to a PC or other work station using a secure localized connection. The PC or workstation to which the HHD may be uplinked/downlinked may have the access software therein, or may be connected to the access software that is held in a secure server.

In one embodiment of the invention, the HHD may be initially connected to the PC through a secure localized connection. Identified data, which may be encrypted, is then downloaded to the HHD. In some instances, where additional security is desired as discussed above, the identified data is "flagged" as it is downloaded for deletion from the HHD if the HHD does not comply with certain security rules within a specified predetermined period of time. For example, if the HHD is not synchronized with the PC, or if the HHD's authorized user does not transmit an authorization code to the secure server or PC within the predetermined period of time, the identified data may be marked for automatic deletion from the persistent memory of the HHD. Thus, if such a protocol is utilized in accordance with the present invention, identified data stored in the persistent memory of the HHD will only be available to an unauthorized user thereof for a relatively short period of time following separation of the HHD from the authorized user.

As will be understood by one of ordinary skill in the art, it will be necessary to associate the identified and de-identified data together at some point in time. To accomplish this task, in accordance with the above-identified "key" embodiment, as the identified data is loaded onto the HHD, it may be supplied with an independently generated identifying key that is used to link the identified data with the corresponding de-identified data later on in the process. The identified data may be stored in persistent memory in the HHD wherein it may optionally be retrieved only upon the receipt of a password or other security key, such as a biometric, from the authorized user. Of course any number of additional security features are known to those of ordinary skill in the art and could be incorporated into the HHD or the rest of the system in a manner consistent

with the method of the present invention. The use of these security features provides yet another layer of protection to the identified data stored in the persistent memory in the HHD in that even if the HHD were stolen or lost, access to the identified data stored therein would be difficult to obtain. Furthermore, as discussed previously, such unauthorized access would not be considered to be a major breach of security given the non-confidentiality of the identified data. After downloading of the identified data and the identifying key, the HHD is ready to access new or updated de-identified data corresponding to the identified data stored on the HHD in persistent memory. This access may be accomplished in accordance with the present invention as follows.

First, the new or updated de-identified data may be sent from the originator to a secure server that is controlled by the issuer. When both de-identified and identified data are desired on the HHD, the de-identified data may be sent with a marker, or key, which allows the de-identified data to be correlated with the corresponding identified data. In some instances the marker will be all or some of the identified data, an independently generated key, or the identifying key discussed above. If the marker is the identifying key, then the de-identified data is ready for transmission to the HHD being held by the authorized user immediately. However, if the marker is all or portions of the identified data, or a separate key, the de-identified data must first be supplied with the identifying key corresponding to the identified data held on the HHD. Next, in order to assure the security of the de-identified data that will shortly be transmitted over an over air network, the de-identified data is stripped of the marker. Optionally, the de-identified data may be encrypted to further protect its security. Of course it is to be understood that such encryption is not strictly necessary as the de-identified data should not contain any information that, absent the corresponding identified data, is particularly sensitive. In any event, whether encrypted or not, the de-identified data is now ready for transmission to the HHD.

Accordingly, the de-identified data is then transmitted to the HHD using over air transmission technology. Upon receipt of the new de-identified data at the HHD, a message or other indication may be provided by the HHD that new information is present. If the de-identified data is being sent to an HHD wherein there is no corresponding identified data stored therein, the presentation of the de-identified data to the authorized user completes the transaction. If, however the system is one wherein the authorized user

has access to identified data through the HHD, at that point, the authorized user may be asked to present a password, biometric, etc., in order to view the combined record.

Upon presentation of the appropriate response, the identified database in the HHD is unlocked and, using the identifying key, the corresponding identified data is retrieved. The identified data and de-identified data are then combined for viewing, and in some embodiments, modification by the authorized user. It is to be understood that the display of the combined record on the HHD does not result in the storage of the combined record and that the display thereof is only in non-persistent memory. If modifications to the de-identified data are made by the authorized user, the modifications are sent back to the secure server with the identifying key, but not the identified data, so that the archival copy of the de-identified data may be changed to incorporate the modifications made by the authorized user.

One of ordinary skill in the art will understand that the present invention may be utilized effectively in a "pull" mode as well in the "receive" mode discussed above. The pull mode may be necessary when the authorized user of the HHD desires a specific combined record and has not been notified by the originator that that record has been updated or modified. In order to accomplish this, the desired identified data may be retrieved from the HHD memory as discussed previously and the authorized user may select the combined record to be viewed/modified. Upon retrieval of the identified data, the identifying key only, along with the appropriate request for the corresponding de-identified data, is transmitted to the secure server using over air technology. The secure server then evaluates the request, and, if the request is not in violation of security rules, transmits the desired de-identified data with the corresponding identifying key back to the HHD.

The restricted algorithms used herein to derive various security keys may be any algorithm useful for this purpose including algorithms that are known in the art or newly developed. Preferably, in order to provide increased security, the algorithms are designed anew or modified for each particular application. Of course, the identity of the specific algorithm used in any particular application must be kept confidential or non-public in order to ensure that security is not breached. In any event, the design and use of such security-key generating algorithms in conformance with the present invention is well-known in the art.

In a preferred embodiment of the invention the following process is used to ensure that only an authorized user can re-construct the record: After the access software validates and authenticates a user, a secure channel is created between the access software and the identified data software. The access software requests an access list from the Identified Data Software and presents the authorized user with the access list, which is a list of the records to which the user has access. The authorized user selects a record to open, and the identified data software transmits to the access software the related identified data and ILK. A secure channel between the access software and the de-identified data software is established. The access software transmits to the de-identified software the authorized user access key, the authorized user verification key, the de-identified issuer key (or alternative user and/or issues specific data) and the ILK. The de-identified software uses this information along with the previously mentioned restricted algorithm to create the DILK, and thus associate the related de-identified data. The de-identified software transmits the de-identified data to the access software where it is combined with the identified data for presentation to the user.

In a preferred embodiment, the entity that stores the identified database (the identified data service provider) does not control directly or indirectly the entity that stores the de-identified database (the de-identified data service provider). The converse also is true. The entity that stores the de-identified database does not control directly or indirectly the entity that stores the identified database. In addition; the identified data and the de-identified data are preferably transmitted and stored only in encrypted formats, using different encryption keys for the identified and de-identified data. In addition recognized administrative, physical and technical safeguards instituted at both the identified data service provider and the de-identified data service provider result in enhanced protection. For example, the identified data service provider and the de-identified service provider track historical data on authorized users, their retrieval patterns, issuer policies, and other factors to provide a level of behavior monitoring and terminate service where there is an unexplained variation.

The use of the data storage and retrieval method disclosed herein creates several levels of security thereby making unauthorized access to the sensitive data highly unlikely. For example, to compromise the confidentiality of the data storage databases an unauthorized user would have to obtain at least a portion of the identified data, the de-identified database, the random number used to create the identified linking key, the

algorithm used to create the identified linking key, and the algorithm for creating the de-identified linking key, as well as the encryption key for the identified data and the encryption key for the de-identified data. To compromise the re-construction process, an unauthorized user would have to obtain the authorized user access key, the authorized user verification key, the identification issuer key, the de-identification issuer key, and the restricted algorithms for creating the keys to secure both the communications to the identified data service provider and the communications to the de-identified data service provider. Additionally, the usage tracking facilities would detect unusual usage patterns and terminate the process.

In accordance with the general description set forth above, the present invention provides methods for protecting the privacy, security and integrity of confidential, individually identifiable, personal information and for facilitating the creation, use and access to this information over a secure public or private network or, where applicable, through an HHD. Other objects and advantages will be apparent from the following description, the drawings and the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a schematic diagram of a network and hardware configuration operable in conformance with an embodiment of the method of the present invention;

Fig. 2 is a schematic diagram of a network and hardware configuration operable in conformance with an embodiment of the method of the present invention utilizing an HHD;

Fig. 3 is a schematic system diagram depicting the splitting of identified data and de-identified data in accordance with an embodiment of the method of the present invention;

Fig. 4 is a schematic system diagram depicting the flow of data and linking keys between the DDSP, the IDSP, and the POS in accordance with an embodiment of the invention; and

Fig. 5 is a schematic system diagram depicting the creation and transfer of linking keys in accordance with an embodiment of the invention.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

A preferred embodiment of the present invention is a combination of specific security processes and technology components which fulfill the object of bifurcating and protecting the privacy, security and integrity of confidential, individually identifiable, personal information and for facilitating the creation, use and access to this information over a secure public or private network. As will be understood by one of ordinary skill in the art, many network and hardware configurations could be used to successfully practice the security method of the present invention, the various combinations and permutations thereof being numerous. One configuration is discussed herein with the understanding that additions and variations thereof are possible without departing from the scope of the present invention. As best shown in Figs. 1 and 4, the basic concept of a preferred embodiment of the present invention involves a relatively basic computer network using the technology components discussed below.

Technology Components

There are four major software technology/hardware components that may be utilized in a preferred embodiment of the present invention, namely:

1. Access Software– the software operating at the Point-of-Service (POS).
2. Identified Data (ID) Software – the software operating at the site of the storage and retrieval of the Identified Data (Identified Data Service Provider).
3. De-Identified Data (DID) Software– the software operating within the De-Identified Data Service Provider (DDSP) that manages the storage and retrieval of the De-Identified Data.
4. Workstation/PC network access (PC).

1. The Access Software can provide three primary functions:
    a. Identification and separation of sensitive data into two parts (files): Identified Data File and De-Identified Data File
    b. Establishment of secure communications with both the Identified Data Service Provider (IDSP) and the De-Identified Data Service Provider (DDSP)
    c. Retrieval process and re-construction process for Authorized Users that unites the Identified and De-Identified Data files into a single record.

2. The Identified Data (ID) Software provides four basic functions:
    a. Validation of the Authorized User of the Identified Data Service
    b. Management of the Authorized User Access List – the list of records a specific Authorized User or Authorized Role can access
    c. Storage and retrieval of Identified Data Files (records)
    d. Software to generate the Identified Linking Key (ILK) to index ID Data storage (and retrieval). This ILK is later used as a "seed" to derive the index to the De-Identified Data stored at the DDSP. This software is optional – an Issuer (user of the present invention) can use an existing keying system to provide the ILK or they can create their own.

3. The De-Identified Data Software (DD) provides four basic functions:
    a. Validation of the Authorized User of the DID Service (DDSP)
    b. Management of the DID Authorized User Keys
    c. Storage and retrieval of De-Identified Data Files (records)
    d. Software to generate the De-Identified Linking Key (DILK). This software provides the encryption/decryption of the ILK to the real storage keys for the De-Identified Data (DILK).

4. The Workstation/PC network access (PC) allows the authorized user to access and create records/files.

Other miscellaneous functions that are either provided by the present invention, the Issuer, the Intermediary, or the Point-of-Service are:

a. Issuer key (ID Issuer Keys and DID Issuer Keys) Management – these are the keys that identify the particular organization or institution with which the Authorized User is associated with.
b. Authorized User keys (Authorized User Access Key and Authorized User Verification Key) Management – these are the unique keys that identify the authorized users.
c. Local encryption/decryption of data storage at the ID Data Service. The De-Identified Data Service (DDSP) will use local encryption and decryption of data storage in compliance with the DDSP's operating procedures.

d. Central service (at the DDSP) to manage the criteria for separation of data at the Access Software sites (Points of Service).

The authentication of users and/or issuers can be handled by a separate "third party" authentication server or at the Point-of-Service (in conjunction with the Access Software) can be provided by many means including (but not limited to):

a. Third Party authentication services such as Intel IAS, Verisign, etc.
b. Public Key Infrastructure software such as Entrust
c. Custom security software solutions
d. Existing Issuer security solutions
e. Manual processes

Processes

In practicing the present invention five basic processes are typically involved:

A. User Validation and Access Control
B. Record Separation
C. Linking Key Generation and Control
D. Record Storage
E. Record Re-Construction

Process A - User Validation and Access Control

The first element in the access and use of a preferred embodiment is the creation and maintenance of a user authentication process. Authentication of users of the service can occur at multiple levels:

1) At the Access Software/third party level – validating the Authorized User Access and Verification Keys

The Access Software operates at the Point-of-Service (healthcare facility, insurer, etc.) or a trusted intermediary (web site, third party outsource company, etc.). Each Authorized User of the present invention will typically be provided two pieces of identification (keys) – Authorized User Access Key and the Authorized User Verification Key. The Access Software also will typically hold two important pieces of security information – the Identified

Issuer Key (ID Issuer Key) and the De-Identified Issuer Key (DID Issuer Key).

The user authentication process typically will occur in the following manner. The Authorized User enters the Authorized User Access Key and the Authorized User Verification Key through the PC. Again, this process is defined by the authentication policy stipulated by the Issuer. The Access Software validates Authorized User keys and the basic services are presented to the Authorized User. No data is accessed until secure channels of communication are established.

2) In the secure communications to the Identified Data Service and the secure communications channel to the De-Identified Data Service (DDSP)

The primary mechanism for accessing the sensitive data (re-construction) is through connections over a private or public network (Internet predominately). All information should be sent using encryption to protect the information as it travels between the user and the associated entities (ID Service Provider and DDSP). Different encryption mechanisms with different keys are used when sending information to the different entities for the highest security.

As best shown in Fig. 5, access to a preferred embodiment is provided using a multi-key process. Keys typically derived from the Authorized User Keys, the Issuer Keys (or other user and issuer specific data), and two separate restricted algorithms will typically be used to secure each of two communications channels – secure communications with the Identified Data service and secure communications with the De-Identified Data (DDSP) service.

A channel to the Identified Data is established using an algorithm to modify the Authorized User's Keys and the Identified Data Issuer Key (ID Issuer Key), into a key (Channel Access Key) that is presented to open the secure channel to the Identified Data Service. The creation of the Channel Access Key to secure the communication to the Identified Data Service is accomplished by using the issuing agency key (ID Issuer Key), Authorized User's Access and Verification keys and a restricted algorithm (ID Channel

Key Algorithm). This derived key process occurs within the Access Software and is used to secure the connection to the Identified Data Service Provider.

A channel to the De-Identified Data is established using a separate algorithm to modify the Authorized User's Keys and the De-Identified Data Issuer Key (DID Issuer Key), into a second key (Channel Access Key 2) that is presented to open the secure channel to the De-Identified Data Service (DDSP). The creation of Channel Access Key 2 to secure the communication to the De-Identified Data Service is accomplished by using the issuing agency key (DID Issuer Key), Authorized User's Access and Verification keys and another restricted algorithm (DID Channel Key Algorithm). This derived key process occurs within the Access Software and is used to secure the connection to the De-Identified Data Service Provider.

3) Access to Identified Data and Access to De-Identified Data

Authorized User validation can also occur when access to the ID Data Service Provider is requested. The Authorized User Access Key and Authorized User Verification Key are provided to the ID Data Software and are validated by locating the Authorized User entry in the Access List database. If the Authorized User information does not exist in the Access List, then access is denied. Technically, this access denial should have occurred at the time a request to establish the ID Secure Communication Channel was issued. If invalid Authorized User information had been passed, the secure channel would have never opened to the ID Data Service Provider. This validation is an additional checkpoint for valid (authorized) access to the ID database. If the ID data is stored at the point of service, this user validation process will typically not be warranted.

Authorized User validation occurs, again, when access to the DID Data Service (DDSP) is requested. The Authorized User Access Key and Authorized User Verification Key are provided to the DID Data Service and are validated by locating the Authorized User entry in the DID Key database. If the Authorized User info does not exist in the DID Key database, then access is denied. Again, technically, this Access denial should have occurred at the time a request to establish the DID Secure Communication Channel was

issued. If invalid Authorized User information had been passed, the secure channel would have never opened to the DID Data Service. This validation is an additional checkpoint for valid (authorized) access to the DDSP.

Process B - Data Separation

As best shown in Fig. 3, in accordance with an embodiment of the invention, sensitive data records are separated into two files: a file with the identifying data (Identified Data File – ID File) and the file with the De-Identified Data File (DID File). Optionally, the ID File and DID File could be further sub-divided for added security but that is an implementation detail, whose need is driven by the entity that is providing access to the sensitive data (Issuer). Identification criteria for data separation is defined and maintained by a central service (operated within the DDSP) that manages the Access Software remotely.

As shown in Figs. 1 and 4, after separation of data, the secure communication channel to the Identified Data Service Provider is created. The Authorized User Keys, the ID Issuer Key, and The Identified Data File are then sent to the ID Service Provider. A linking key (Identified Linking Key), which is a master index used for the storage of the Identified Data File and is a parameter for generating the linking key (DILK) used to index and store data at the De-Identified Data Service Provider (DDSP), is created at the Identified Data storage point (ID Service Provider) by the Identified Data software and used to control access and storage of Identified Data.

A preferred embodiment will provide a software tool to create the Identified Linking Key (ILK) but, alternatively, the entity storing the identified data (Identified Data Service Provider) could use an existing or different process for indexing and storing the Identified Data.

The ILK is returned to the Access Software and a secure communications channel is opened to the De-Identified Data Service Provider (DDSP). The De-Identified Data File, the Authorized User Keys, the De-Identified Data Issuer Key, and the ILK are sent to the DDSP. There, the DID Service creates a De-Identified Linking Key (DILK) and stores the data. The status of the transaction (success or failure code) is returned to the Access Software and reported to the Authorized User.

Process C - Linking Key Generation and Control

The Identified Linking Key can be provided by an existing or newly created algorithm at the Identified Data Service Provider or by a software component provided by the DDSP. In a preferred embodiment, the ILK Generation Software (software tool) will generate the Linking Key (ILK). The ILK will be created using a random key generation process that creates unique keys.

In one embodiment, the ILK Generation Software will create the ILK using components of:

1. A key (Identified Issuer Key) that is specific to the issuer.
2. A random number
3. The Authorized User Access Key. The Authorized User Access Key is the first key that is entered (manually or automatically) by the Authorized User of the sensitive data. The Issuer, specifically, the security processes and policies of the particular Issuer organization determine the source and input process of this key.
4. The Authorized User Verification Key. The second key entered by the Authorized User to verify identity. Again, the Issuer, specifically, the security processes and policies of the particular Issuer organization determine the source and input process of this key.

Those skilled in the art will recognize that other user and/or issuer specific data could be used to create the ILK. A restricted algorithm is used for deriving the ILK from the components of the key. The ILK is used as the index for the record storage in the Identified Data Service Provider database.

An Access List associated with the Authorized User is updated in the Authorized User Access List Database. This list includes the Authorized User Key and an associated list of ILK's that the Authorized User controls. Optionally, other security models (such as role-based security) can be employed to extend the access and/or update of records under control of the Authorized Users to other Authorized Users with a "need to know". This would provide for the ability of a nurse, administrator, etc. to have authorized access to a set of appropriate records (an Authorized Role).

The key created at the time of separation (the ILK that is used to store the Identified Data) is transmitted back to the Access Software. The ILK and the De-

Identified Data File (DID File) are transmitted over a secure channel to the DDSP. The data is transmitted securely over the private or public network (Internet predominately) to the DDSP and stored using an additional restricted process to "transform" the linking key used for storage of the data. The original key (ILK transmitted with the De-Identified Data) is erased and never stored. The De-Identified Data itself is encrypted using a restricted algorithm so that the De-Identified Data File is never stored in clear text format inside the DDSP.

In a preferred embodiment, the process for "encrypting" the linking key is a combination of the DID Issuer's Key (different from the issuer's key used at the point of service for the Identified Linking Key generation), and a restricted transformation algorithm. The transformed linking key (De-Identified Linking Key – DILK) is used to index the storage of De-Identified Data in the DDSP database.

Process D - Data Storage

Data (Identified and De-Identified) may be stored in two physically separate locations. Identified Data should be held either at the Point-of-Service (healthcare facility, office, insurer, etc.) or at a trusted intermediary (a web site such as WebMD, an insurer's site, a recognized industry expert, etc.). In either embodiment, the Identified Data is held close to the Point of Service – and called the Identified Data Service Provider. Identified Data would be locally encrypted using a key defined and held at the Identified Data Service Provider.

The De-Identified Data is held at a De-Identified Service Provider (DDSP), along with the key management facilities. De-Identified Data is stored encrypted (using a local restricted encryption key and process) and linked using a "transformed" linking key algorithm.

To compromise a patient record (or any other sensitive data record), a would-be thief would have to obtain a copy of the Identified Data (or entire database), a copy of the De-Identified database, the knowledge of the algorithm to create the Identified Linking Key, the algorithm for "transforming" the Identified Linking Key into the "transformed" version (De-Identified Linking Key) used to index the De-Identified data, the local encryption key used for the storage of De-Identified Data, and the local encryption key used for storing the Identified Data. This would be a very daunting and nearly

improbable scenario, thus providing privacy and security of the sensitive data being managed by the present invention.

Process E - Data Re-Construction

Again, the primary mechanism for accessing the sensitive data (re-construction) is over secure private or public network (Internet predominately) connections. All information is sent using encryption to protect the information as it travels between the authorized user and the associated data service provider entities. Different encryption mechanisms with different keys are used when sending information to the different entities for the highest security.

The Authorized User is validated and authenticated by the Access Software and a secure channel to the Identified Data is established following those two processes, previously mentioned.

Once the secure channel is opened to the Identified Data Service Provider, the Authorized User Keys are, again, validated and the records available to that Authorized User or the Authorized User's role are indexed and presented back to the Authorized User for selection. The index will provide minimal data to support the Authorized User's selection process e.g. name, address, and social security number. Once the Authorized User selects a record to open, a request is sent to the Identified Data Service Provider to return all remaining Identified Data and the Identified Linking Key for the purpose of locating the De-Identified Data.

A secure channel to the De-Identified Data Service is established using the previously mentioned process. The Authorized User's Keys and the DID Issuer Key are presented to the secure channel to the DDSP along with the ILK for the particular record being requested. The Authorized User is validated for access.

The restricted algorithm for "transforming" the Identified Linking Key into the De-Identified Linking Key is applied and used as the index into the De-Identified Data database. The associated data is decrypted locally and transmitted back to the Access Software. The Access Software at Point of Service combines the Identified record and the De-Identified record to provide the Authorized User with the complete set of sensitive data.

To compromise this Re-Construction (communication) process, a would-be thief would have to obtain the Authorized User Keys, the Issuer Keys, and the present

invention process for modifying the keys to secure both of the communications channels. Additionally, intelligence in the DDSP would maintain historical data on authorized users, their retrieval patterns, issuer policies, and other factor to provide a level of behavior monitoring. This is very similar to the strategies employed in the financial industry to monitor credit card usage, check usage, etc. to detect unusual usage patterns and potential fraud. This same level of service would be in place to monitor and track access and usage patterns of authorized users. In the event of a highly improbable event in which the Access Keys are compromised, the usage/fraud tracking should trigger and stop the ability of the would-be thief to secure more than a few records before the keys would be revoked and the process stopped. While this in itself would still be a significant risk event, it still would limit the damage to only a few records and lessen the amount of damage that could be accomplished in one break-in.

As mentioned previously, the method of the present invention can also be accomplished in accordance with the use of an HHD to provide flexibility in the secure creation and receiving of sensitive data. Such an embodiment is best shown in Fig. 2. In this regard, it is noted that various network connections used in this embodiment may have widely varying levels of security depending on the transmission technique, the degree of encryption of the transmitted information, etc. Of course, while it is generally desired to use connections that are as secure as convenience and expense will allow, the most secure connections, such as hard-wired, dedicated secure connections, are not always available.

Accordingly, the security method disclosed herein in connection with the use of an HHD may operate on a secure basis even when none of the enumerated connections are absolutely secure as long as the POS remains impenetrable to breaches in security. Furthermore, it is to be generally understood that in the context of the present invention the connection between the transmission intermediary and the HHD will be an over air connection, and therefore relatively insecure by its very nature. Of course, as discussed herein, the present invention takes this over air insecure connection into account and therefore the relative insecurity of this specific connection does not compromise the security and integrity of the information viewed, modified and transmitted from an HHD used in accordance with the present invention.

In accordance with an embodiment of the invention, identified data may be loaded on an HHD from the POS through the PC, preferably through a secure,

localized connection, such as a wired, or wireless "bluetooth"-type, connection. The identified data may be encrypted on the HHD to provide an extra measure of security if the HHD is lost or stolen. To provide further security, the identified data may be flagged to be deleted if it is not updated during an institutionally determined period of time. For example, if the HHD is not physically synchronized with the POS through the PC every 24 hours, then the identified-data is deleted from the HHD memory. Thus, even if the HHD were lost, an unauthorized user thereof would have to break into the encrypted identified data within the allocated period of time. Of course, even if that were accomplished, it would not be considered a major security breach in that the unauthorized user would only obtain a list of relatively innocuous patient identifying information (e.g. names, addresses, etc.).

In accordance with an embodiment of the invention, when an update to clinical (de-identified) data is made by an originator of the data (for example, lab results are completed for a patient), the originator sends the update to the POS from the DDSP. The de-identified data may be sent from the originator to the POS with a marker, or key, which allows the de-identified data to be correlated with the corresponding identified data. In some instances the marker will be all or some of the identified data, an independently generated key, or the identifying key discussed above. If the marker is the identifying key, or if the de-identified data is being sent without a marker (as may be desirable in some instances) then the de-identified data is ready for transmission to the HHD immediately. However, if the marker is all or portions of the identified data, or a separate key, the de-identified data must first be supplied with the identifying key corresponding to the correlating identified data held on the HHD. Next, in order to assure the security of the de-identified data that will shortly be transmitted over an insecure network, the de-identified data is stripped of the marker. Optionally, the de-identified data may be encrypted to further protect the security thereof.

Next, the de-identified data and the identifying key are transmitted to the transmission intermediary (which may be a cellular tower, a broadcast antenna, etc.). The transmission intermediary, acting generally only as a relay of information, passes the de-identified information and, where applicable, the identifying key (marker) over an over air connection to the HHD. When the de-identified data is received by the HHD, the authorized user thereof is notified that new de-identified data is present. The

authorized user may then be requested to enter authenticating information (e.g. password, biometrics, etc.) into the HHD. Upon receipt of the acceptable authentication, the HHD temporarily unlocks the encrypted database of identified data and obtains the identified data corresponding to the de-identified data just received using the identifying key sent with the de-identified data. Then the identified and de-identified data are merged in order to display the combined record, including the update, to the authorized user.

At this point the identified database in the HHD may be re-locked, and the combined record is only used for display on the HHD in non-persistent memory. If the application allows for the authorized user to respond to the update, the authorized user enters whatever information is appropriate, and the new de-identified data (and only the new de-identified data) is then sent, along with the identifying key, to the POS. At the POS, the identifying key is used to archive the new de-identified data with the originator of the de-identified data (generally at the DDSP).

The present invention may also be used successfully in a pull mode wherein the authorized user of the HHD desires to review a specific combined record. In this case, the authorized user enters the authenticating information and is enabled to view the identified database including a list of patients. An identified data record is selected, and the request for the necessary de-identified data corresponding thereto is made. From the HHD the request, along with the appropriate identifying key, is sent to the POS along with an appropriate request code. As in the update case described above, the identifying key is used to obtain the necessary de-identified data, and the de-identified data is retrieved from the DDSP.

Additional levels of security can be incorporated through the POS in accordance with embodiments of the present invention as discussed above. For example, the POS can log an audit trail of all accesses and updates to identified and de-identified data. When doing so, rules can be applied to look for and flag unusual or suspicious access patterns. Also, access can be restricted such that authorized users are allowed access to only a single record at a time. In addition, certain reasonable timeframes can be applied so that a rogue system requesting one record after another can be detected. "Landmine" data (that is, data and users which do not exist) can be inserted in the

system to flag users requesting data sequentially. Other well-known safeguards and procedures are available and would add additional levels of security. However, their implementation herein would be considered obvious to one of ordinary skill in the art and accordingly have not been specifically delineated.

Having described the invention in detail, it will be apparent that modifications and variations are possible without departing from the scope of the invention defined in the appended claims.

What is claimed is:

CLAIMS

1. A method for protecting confidential data records comprising the steps of:

separating a record into first and second files;

generating a first key associated with said first file;

storing said first file and said first key in a first database;

transmitting said second file and said first key over a network for storage in a second database;

generating a second key derived from said first key and associating said second key with said second file; and

storing said second file in a second database using said second key to index said second file.

2. The method of claim 1 wherein the method includes the additional step of reconstructing said record from said first file and said second file in response to a request from an authorized user.

3. The method of claim 1 wherein said first file is encrypted prior to storage.

4. The method of claim 1 wherein said second file is encrypted prior to storage.

5. The method of claim 1 wherein said network is the Internet.

6. The method of claim 2 wherein said first file includes identification data and said second file includes de-identified data.

7. The method of claim 1 wherein said first and second databases are stored at physically separate facilities.

8. The method of claim 6 wherein the entity that stores said first database does not directly or indirectly control the entity that stores said second database.

9. The method of claim 1 where the method includes the additional step of transmitting said first file over a network for storage in said first database.

10. A method of claim 9 wherein said transmission of first and second files is tracked and usage patterns are compared to detect unauthorized access.

11. The method of claim 1 wherein the data records are health care records.

12. The method of claim 1 wherein the step of generating the first key is carried out on a first computer which stores the first database and the step of generating the second key is carried out on a second computer which stores the second database.

13. The method of claim 2 wherein said authorized user is authenticated prior to re-construction of said record.

14. The method of claim 13 wherein said authentication is performed at a point-of-service provider.

15. The method of claim 13 wherein said authentication is performed by a third party authentication service.

16. A method for providing access to sensitive data on a personal electronic handheld device in a secure manner comprising the steps of:
separating a record into first and second files;
storing said first file in a first database;
storing said second file in a second database;
downloading said first file to a portable peripheral;
transmitting said second file over an over air network to said portable peripheral;
retrieving said first file from said portable peripheral;
creating a combined record by associating said first file and said second file; and
displaying said combined record on said portable peripheral in non-persistent memory.

17. The method of claim 1 further comprising generating an identifying key and storing said key with said first and second files in said databases and using said key to associate said first and second files to create said combined record.

18. The method of claim 1 wherein said first file is encrypted prior to storage.

19. The method of claim 1 wherein said first file includes identified data and said second file includes de-identified data.

20. The method of claim 1 wherein said second file is encrypted prior to transmission.

21. The method of claim 1 wherein said files contain clinical health care data.

22. A method for providing access to sensitive data on a personal electronic handheld device in a secure manner comprising the steps of:
generating sensitive de-identified data;
downloading said de-identified data to a point of service provider;
transmitting said de-identified data from said point of service provider to a transmission intermediary;
relaying said de-identified data from said transmission intermediary to a personal electronic handheld device; and
displaying said de-identified data on said portable electronic handheld device in non-persistent memory.

23. The method of claim 22 further comprising the steps of downloading identified data files to said personal electronic handheld device and correlating a file from said identified data with said de-identified data using a marker transmitted therewith to create a combined data record.

24. A method for providing access to sensitive data on a personal electronic handheld device in a secure manner comprising the steps of:
generating sensitive de-identified data;
downloading said de-identified data to a point of service provider;

transmitting said de-identified data from said point of service provider to a transmission intermediary;

relaying said de-identified data from said transmission intermediary to a personal electronic handheld device; and

displaying said de-identified data on said portable electronic handheld device in non-persistent memory.

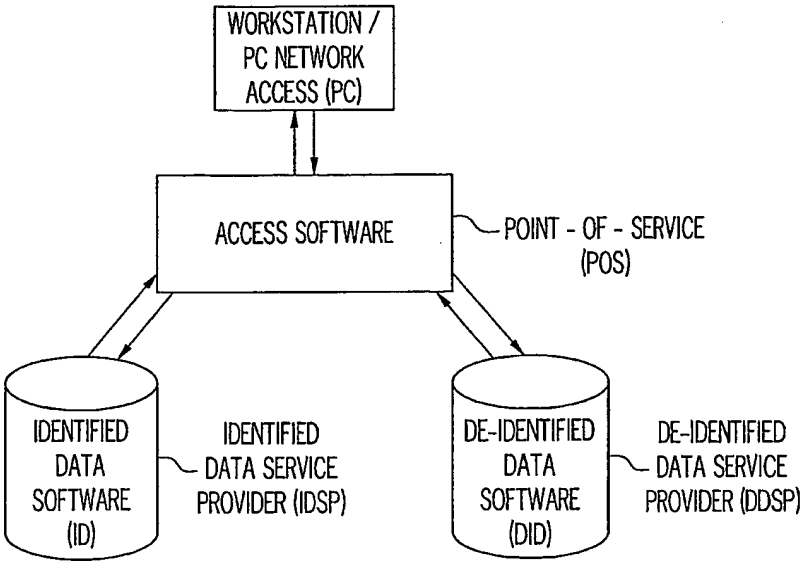
WORKSTATION / PC NETWORK ACCESS (PC)
ACCESS SOFTWARE
POINT - OF - SERVICE (POS)
IDENTIFIED DATA SOFTWARE (ID)
IDENTIFIED DATA SERVICE PROVIDER (IDSP)
DE-IDENTIFIED DATA SOFTWARE (DID)
DE-IDENTIFIED DATA SERVICE PROVIDER (DDSP)

FIG. 1

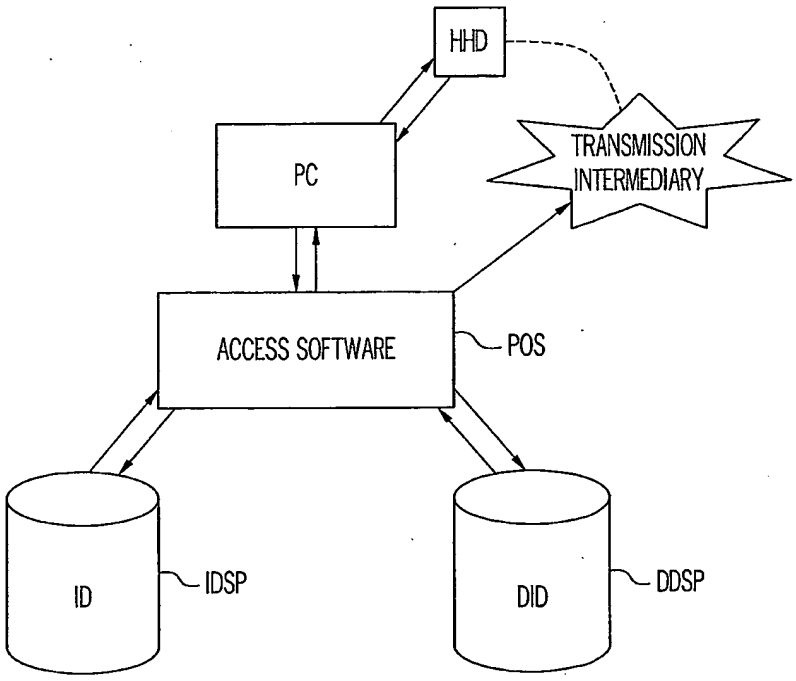
HHD
PC
TRANSMISSION INTERMEDIARY
ACCESS SOFTWARE
POS
ID
IDSP
DID
DDSP

FIG. 2

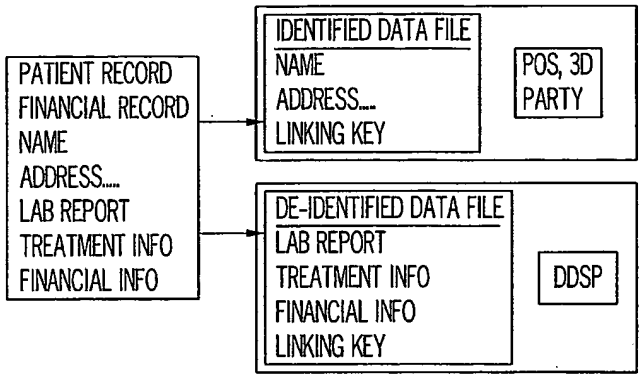
PATIENT RECORD
FINANCIAL RECORD
NAME
ADDRESS....
LAB REPORT
TREATMENT INFO
FINANCIAL INFO
IDENTIFIED DATA FILE
NAME
ADDRESS....
LINKING KEY
POS, 3D PARTY
DE-IDENTIFIED DATA FILE
LAB REPORT
TREATMENT INFO
FINANCIAL INFO
LINKING KEY
DDSP

FIG. 3

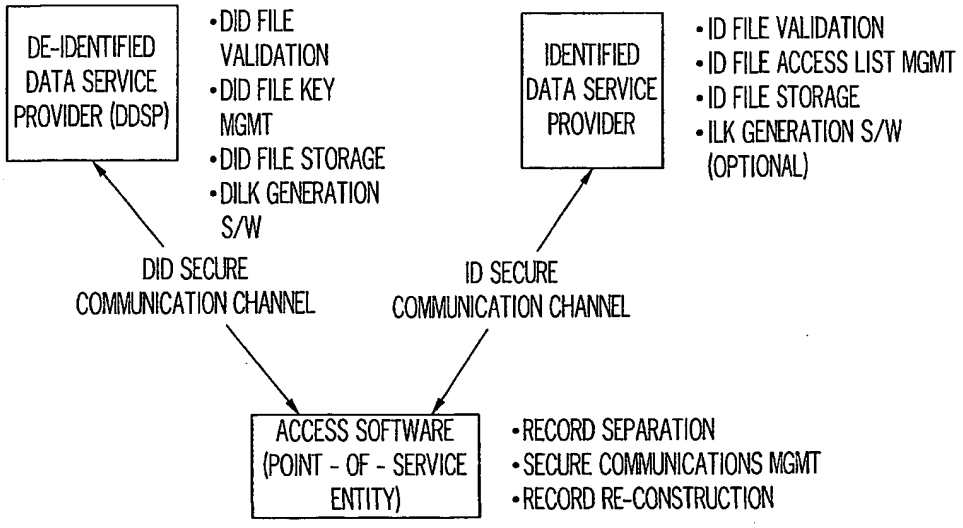
DE-IDENTIFIED DATA SERVICE PROVIDER (DDSP)
•DID FILE VALIDATION
•DID FILE KEY MGMT
•DID FILE STORAGE
•DILK GENERATION S/W
IDENTIFIED DATA SERVICE PROVIDER
•ID FILE VALIDATION
•ID FILE ACCESS LIST MGMT
•ID FILE STORAGE
•ILK GENERATION S/W (OPTIONAL)
DID SECURE COMMUNICATION CHANNEL
ID SECURE COMMUNICATION CHANNEL
ACCESS SOFTWARE (POINT - OF - SERVICE ENTITY)
•RECORD SEPARATION
•SECURE COMMUNICATIONS MGMT
•RECORD RE-CONSTRUCTION

FIG. 4

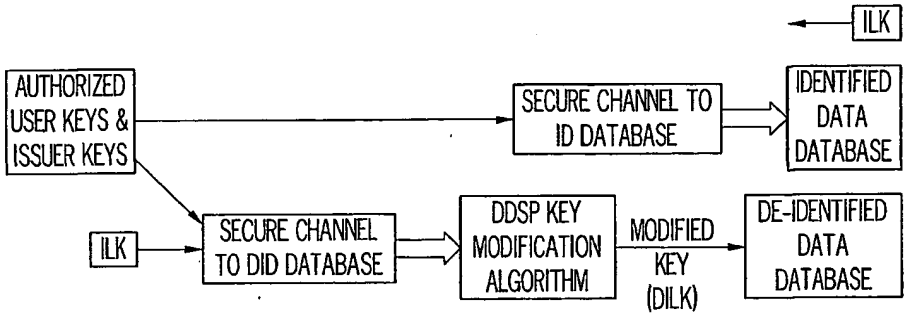
ILK
AUTHORIZED USER KEYS & ISSUER KEYS
SECURE CHANNEL TO ID DATABASE
IDENTIFIED DATA DATABASE
ILK
SECURE CHANNEL TO DID DATABASE
DDSP KEY MODIFICATION ALGORITHM
MODIFIED KEY (DILK)
DE-IDENTIFIED DATA DATABASE

FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/22089

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :Please See Extra Sheet.
US CL :Please See Extra Sheet.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/200, 201, 202, 189, 193; 705/1, 2, 3, 50, 51, 64; 707/1, 9; 711/163, 164

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,012,144 A (PICKETT) 04 JANUARY 2000, SEE ENTIRE DOCUMENT	1-24
A,P	US 6,249,869 B1 (DRUPSTEEN ET AL) 19 JUNE 2001, SEE ENTIRE DOCUMENT	1-24
A	US 5,826,245 A (SANDBERG-DIMENT) 20 OCTOBER 1998, SEE ENTIRE DOCUMENT	1-24
A,P	US 6,199,165 B1 (GRUNNER) 06 MARCH 2001, SEE ENTIRE DOCUMENT	1-24

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 14 SEPTEMBER 2001	Date of mailing of the international search report 19 NOV 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GAIL HAYES Peggy Harrod Telephone No. (703) 305-9618

Form PCT/ISA/210 (second sheet) (July 1998)★

INTERNATIONAL SEARCH REPORT

In [redacted] nal application No.
PCT/US01/22089

A. CLASSIFICATION OF SUBJECT MATTER:
IPC (7):

G06F 7/00, 11/30, 12/14, 17/30, 17/60; H04K 1/00; H04L 9/00, 9/32

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

713/200, 201, 202, 189, 193; 705/1, 2, 3, 50, 51, 64; 707/1, 9; 711/163, 164

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

BRS (FILES: USPAT, EPO, JPO, DERWENT, US PG PUBS, IBM TDBs), DIALOG (FILES: ELECTRON, SOFTWARE, COMPSCI)

search terms: divide, dividing, divided, seperate, seperated, seperating, seperation, split, splitting, splitted, data, information, entity, media, entry, file, content, document, record, key, first, additional, different, hhd, pda, hand held, portable, device